ABSTRACT OF THE DISCLOSURE

[0104] Embodiments of the present invention provide techniques for monitoring a database system for anomalous activity. User behavior information relative to a subject database being monitored may be automatically collected, analyzed and compared with one or more policies to detect anomalous activity. Embodiments collect user behavior data regarding the subject database from a variety of sources, including an audit trail and dynamic views in cooperation with the database management system of the database. Embodiments employ one or more of statistics-based intrusion detection (SBID) and rule-based intrusion detection (RBID) to detect anomalous database activity. If suspicious database access that deviate from the normal usage pattern are detected, a targeted operation, such as alerting the responsible security officers, generating reports, email alerts or the like, is performed.